Monitor

Monitor mode

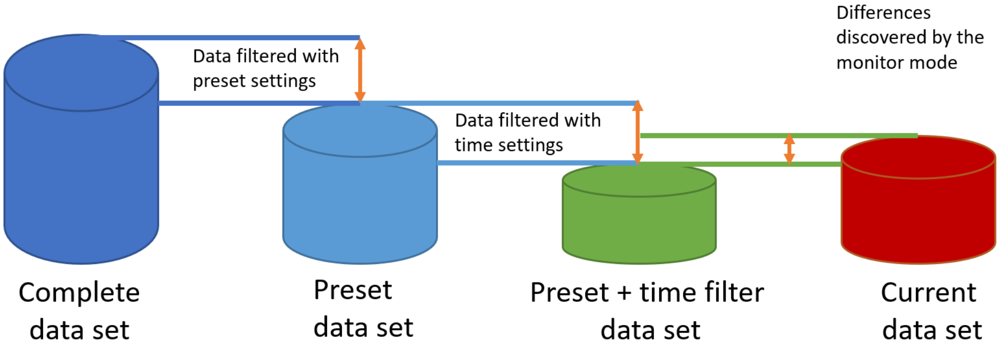
Cisco Cyber Vision provides a monitoring tool called the Monitor mode to detect changes inside industrial networks. Because a network architecture (PLC, switch, SCADA) is constant and its behaviors tend to be stable over time, an established and configured network is predictable. However, some behaviors are unpredictable and can even compromise a network's operation and security. The Monitor mode aims to show the evolution of a network's behaviors, predicted or not, based on presets. Changes, either normal or abnormal, are noted as differences in the Monitor mode when a behavior happens. Using the Monitor mode is particularly convenient for large networks as a preset shows a network fragment and changes are highlighted and managed separately, in the Monitor mode's views.

Baselines as Preset's normal states

A Preset is a set of criteria which aims to show a detailed fragment of a network. To start monitoring a network, you need to pick up a preset, and to define what would be its normal, stable state. This will represent the preset's baseline. A state may rely on a period, as a network fragment may be subject to several states. Hence, it is possible to create several planned, controlled and time-framed baselines per preset, and to monitor the whole network. For example, a normal state of the network can be a typical weekday operating mode, in which numerous processes are performed iteratively. During weekends, these processes may be slowed down, different, or even stopped. Any network phase can be saved as a baseline by selecting the time span in which it occurs, and monitored. Other examples of baselines can be a regular maintenance period, a degraded mode, a weekend and night mode, and so forth. A baseline is created for a situation considered as part of a normal operating process in which all network behaviors (components, activities, properties, tags, variable accesses) will be taken into account for review.

Review and assignment of differences

A difference is a new or changed behavior happening within a fragment of a network. Any difference detected is highlighted in the Monitor mode through several views such as a map, a component list and an activity list. When reviewing these, they can be acknowledged or reported. It depends on whether you consider them as normal or not, and their level of criticality. That is, you can include these changes into your baseline if it is part of a normal network development process, or take action in case of suspicious behavior. By doing so, each baseline will be refined bit by bit over time and become more compliant with your needs.


Differences discovered by the monitor mode
Data filtered with preset settings
Data filtered with time settings
Complete data set
Preset data set
Preset + time filter data set
Current data set

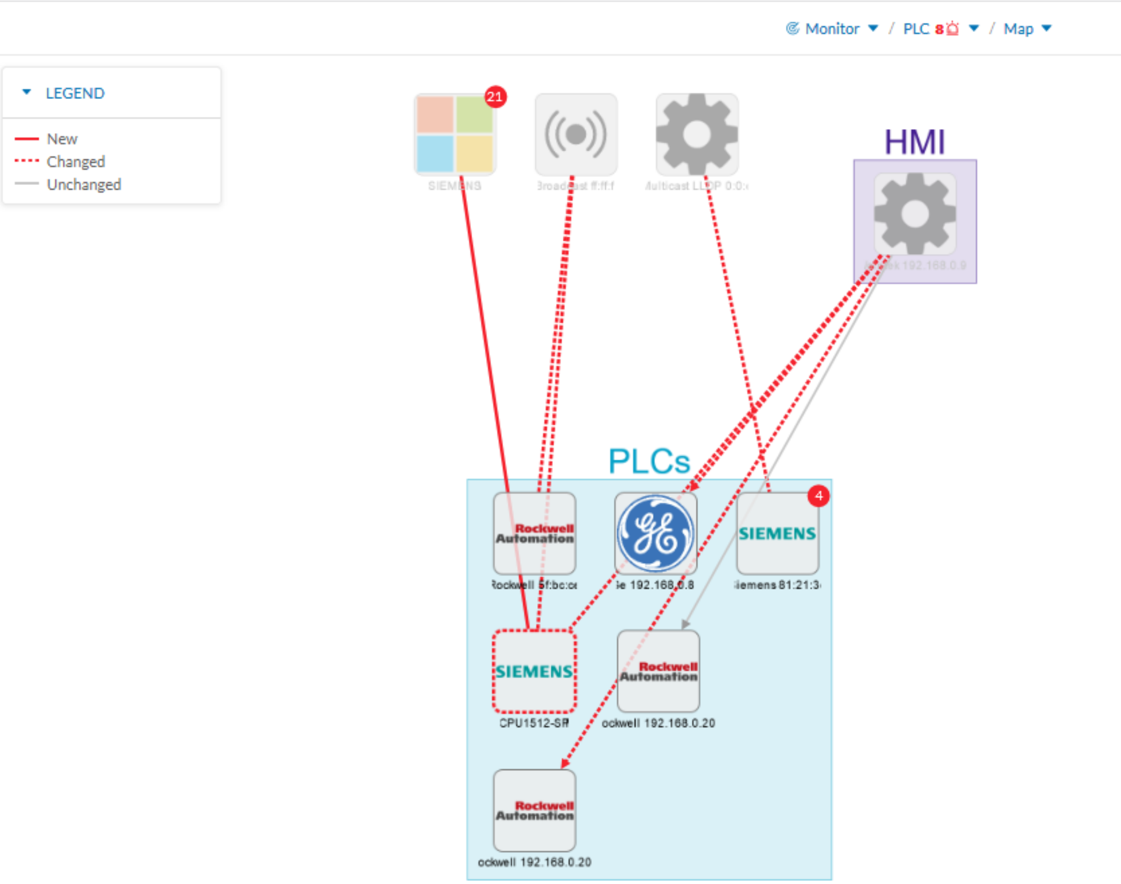
Monitor mode's views

Like in the Explore mode, the Monitor mode offers several views of data so you can see them through different representations. The difference, though, is that in the Monitor mode views new and changed detected elements are highlighted in red.

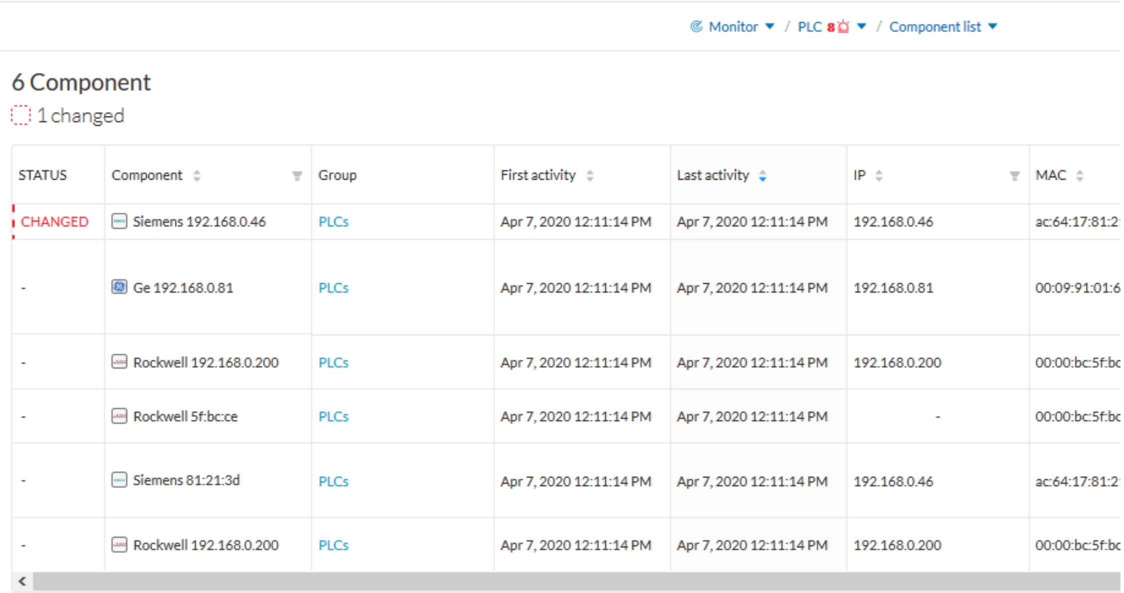
For more information about the views listed below, refer to the Explore chapter.

The map view:

non-aggregated components



The component list view:

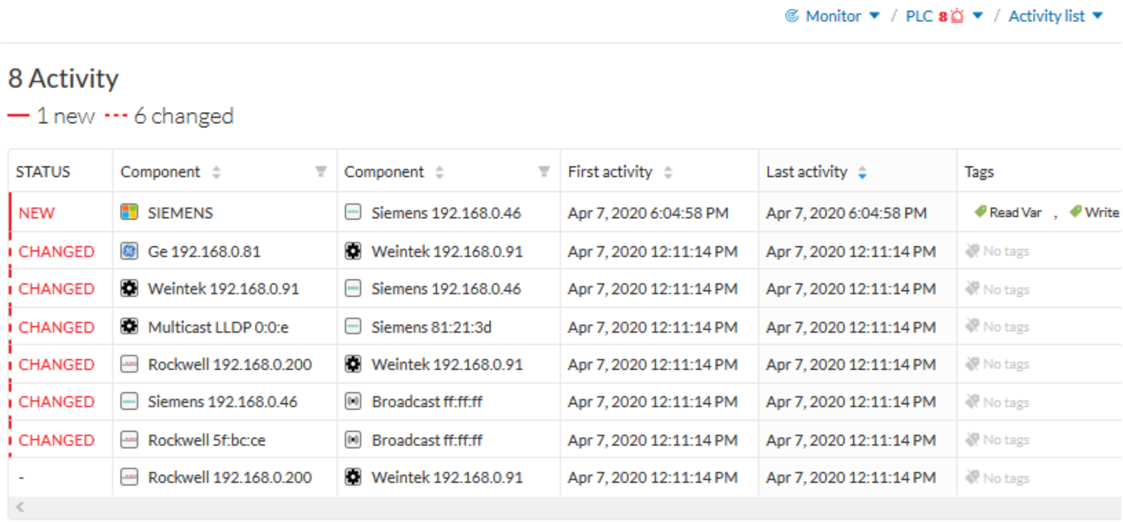


6 Component

1 changed

STATUS	Component	Group	First activity	Last activity	IP	MAC
CHANGED	Siemens 192.168.0.46	PLCs	Apr 7, 2020 12:11:14 PM	Apr 7, 2020 12:11:14 PM	192.168.0.46	ac:64:17:81:2
-	Ge 192.168.0.81	PLCs	Apr 7, 2020 12:11:14 PM	Apr 7, 2020 12:11:14 PM	192.168.0.81	00:09:91:01:6
-	Rockwell 192.168.0.200	PLCs	Apr 7, 2020 12:11:14 PM	Apr 7, 2020 12:11:14 PM	192.168.0.200	00:00:bc:5f:bc
-	Rockwell 5f:bc:ce	PLCs	Apr 7, 2020 12:11:14 PM	Apr 7, 2020 12:11:14 PM	-	00:00:bc:5f:bc
-	Siemens 81:21:3d	PLCs	Apr 7, 2020 12:11:14 PM	Apr 7, 2020 12:11:14 PM	192.168.0.46	ac:64:17:81:2
-	Rockwell 192.168.0.200	PLCs	Apr 7, 2020 12:11:14 PM	Apr 7, 2020 12:11:14 PM	192.168.0.200	00:00:bc:5f:bc

The activity list view:



8 Activity

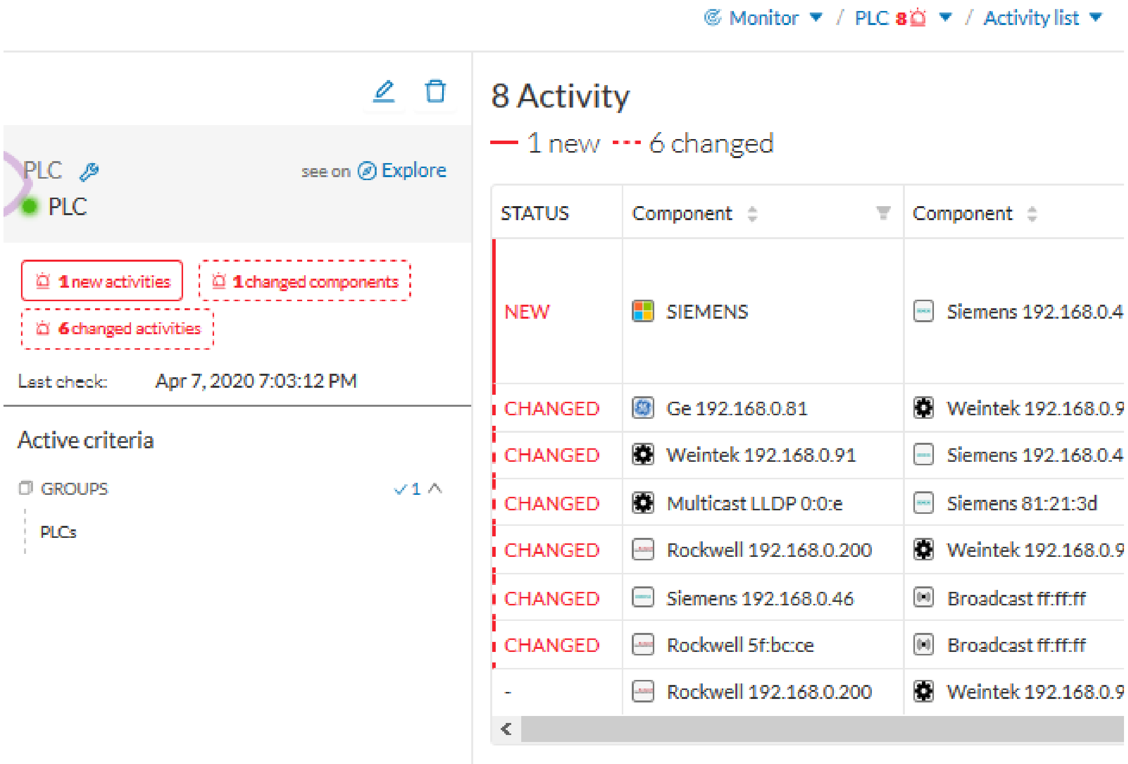
— 1 new ··· 6 changed

STATUS	Component	Component	First activity	Last activity	Tags
NEW	SIEMENS	Siemens 192.168.0.46	Apr 7, 2020 6:04:58 PM	Apr 7, 2020 6:04:58 PM	Read Var , Write
CHANGED	Ge 192.168.0.81	Weintek 192.168.0.91	Apr 7, 2020 12:11:14 PM	Apr 7, 2020 12:11:14 PM	No tags
CHANGED	Weintek 192.168.0.91	Siemens 192.168.0.46	Apr 7, 2020 12:11:14 PM	Apr 7, 2020 12:11:14 PM	No tags
CHANGED	Multicast LLDP 0:0:e	Siemens 81:21:3d	Apr 7, 2020 12:11:14 PM	Apr 7, 2020 12:11:14 PM	No tags
CHANGED	Rockwell 192.168.0.200	Weintek 192.168.0.91	Apr 7, 2020 12:11:14 PM	Apr 7, 2020 12:11:14 PM	No tags
CHANGED	Siemens 192.168.0.46	Broadcast ff:ff:ff	Apr 7, 2020 12:11:14 PM	Apr 7, 2020 12:11:14 PM	No tags
CHANGED	Rockwell 5f:bc:ce	Broadcast ff:ff:ff	Apr 7, 2020 12:11:14 PM	Apr 7, 2020 12:11:14 PM	No tags
-	Rockwell 192.168.0.200	Weintek 192.168.0.91	Apr 7, 2020 12:11:14 PM	Apr 7, 2020 12:11:14 PM	No tags

In any view, on the left side, there is:

- a fixed panel with a summary of the elements that have been detected in the Monitor mode,
- the last time this baseline has been checked,
- the preset it belongs to along with the list of criteria selected.

You can also modify the baseline settings. And the Explore button redirects you to the corresponding preset in the Explore mode.



Monitor ▼ / PLC 8 ▼ / Activity list ▼

PLC

PLC

see on Explore

1 new activities

1 changed components

6 changed activities

Last check: Apr 7, 2020 7:03:12 PM

Active criteria

GROUPS ✓1

PLCs

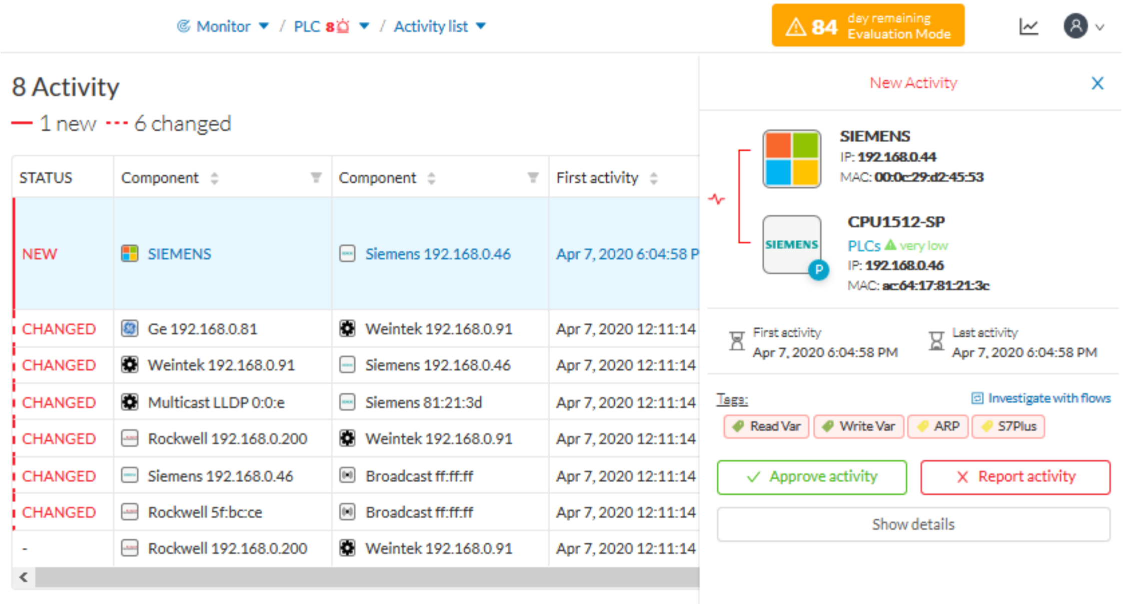
8 Activity

1 new 6 changed

STATUS	Component	Component
NEW	SIEMENS	Siemens 192.168.0.4
CHANGED	Ge 192.168.0.81	Weintek 192.168.0.9
CHANGED	Weintek 192.168.0.91	Siemens 192.168.0.4
CHANGED	Multicast LLDP 0:0:e	Siemens 81:21:3d
CHANGED	Rockwell 192.168.0.200	Weintek 192.168.0.9
CHANGED	Siemens 192.168.0.46	Broadcast ff:ff:ff
CHANGED	Rockwell 5f:bc:ce	Broadcast ff:ff:ff
-	Rockwell 192.168.0.200	Weintek 192.168.0.9

In any view, if you click one of the elements, for example below the activity marked as new in the activity list, a right side panel opens. It gives you:

- information about the activity such as the two components it belongs to,
- the date of the first and the last activity,
- its tags,
- buttons to perform several Review differences.



8 Activity

— 1 new ··· 6 changed

STATUS	Component	Component	First activity
NEW	SIEMENS	Siemens 192.168.0.46	Apr 7, 2020 6:04:58 P
CHANGED	Ge 192.168.0.81	Weintek 192.168.0.91	Apr 7, 2020 12:11:14
CHANGED	Weintek 192.168.0.91	Siemens 192.168.0.46	Apr 7, 2020 12:11:14
CHANGED	Multicast LLDP 0:0:e	Siemens 81:21:3d	Apr 7, 2020 12:11:14
CHANGED	Rockwell 192.168.0.200	Weintek 192.168.0.91	Apr 7, 2020 12:11:14
CHANGED	Siemens 192.168.0.46	Broadcast ff:ff:ff	Apr 7, 2020 12:11:14
CHANGED	Rockwell 5f:bc:ce	Broadcast ff:ff:ff	Apr 7, 2020 12:11:14
-	Rockwell 192.168.0.200	Weintek 192.168.0.91	Apr 7, 2020 12:11:14

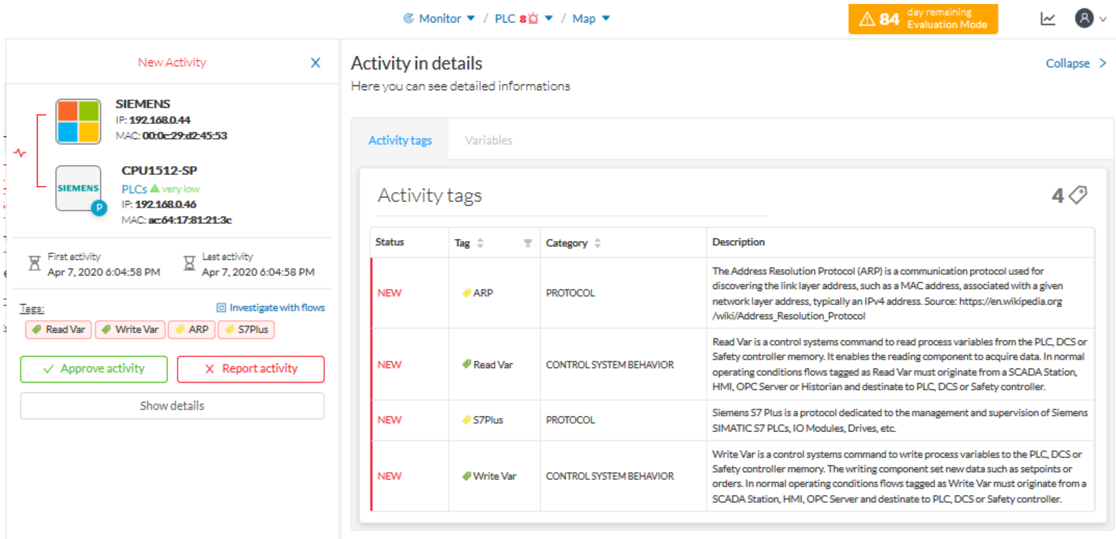
SIEMENS
IP: 192.168.0.44
MAC: 00:0c:29:d2:45:53

CPU1512-SP
PLCs very low
IP: 192.168.0.46
MAC: ac:64:17:81:21:3c

First activity Apr 7, 2020 6:04:58 PM
Last activity Apr 7, 2020 6:04:58 PM

Tags: Read Var, Write Var, ARP, S7Plus

Clicking the Show details buttons opens a window on top with more information, in the example below, it shows the activity tags with the category they belong to and their description.



Activity in details

Here you can see detailed informations

SIEMENS
IP: 192.168.0.44
MAC: 00:0c:29:d2:45:53

CPU1512-SP
PLCs very low
IP: 192.168.0.46
MAC: ac:64:17:81:21:3c

First activity Apr 7, 2020 6:04:58 PM
Last activity Apr 7, 2020 6:04:58 PM

Tags: Read Var, Write Var, ARP, S7Plus

Activity tags 4

Status	Tag	Category	Description
NEW	ARP	PROTOCOL	The Address Resolution Protocol (ARP) is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given network layer address, typically an IPv4 address. Source: https://en.wikipedia.org /wiki/Address_Resolution_Protocol
NEW	Read Var	CONTROL SYSTEM BEHAVIOR	Read Var is a control systems command to read process variables from the PLC, DCS or Safety controller memory. It enables the reading component to acquire data. In normal operating conditions flows tagged as Read Var must originate from a SCADA Station, HMI, OPC Server or Historian and destinate to PLC, DCS or Safety controller.
NEW	S7Plus	PROTOCOL	Siemens S7 Plus is a protocol dedicated to the management and supervision of Siemens SIMATIC S7 PLCs, IO Modules, Drives, etc.
NEW	Write Var	CONTROL SYSTEM BEHAVIOR	Write Var is a control systems command to write process variables to the PLC, DCS or Safety controller memory. The writing component set new data such as setpoints or orders. In normal operating conditions flows tagged as Write Var must originate from a SCADA Station, HMI, OPC Server and destinate to PLC, DCS or Safety controller.

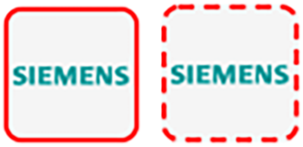
Click the collapse button to come back to the initial view.

However, to go deeper into analysis, click the Investigate with flows button.

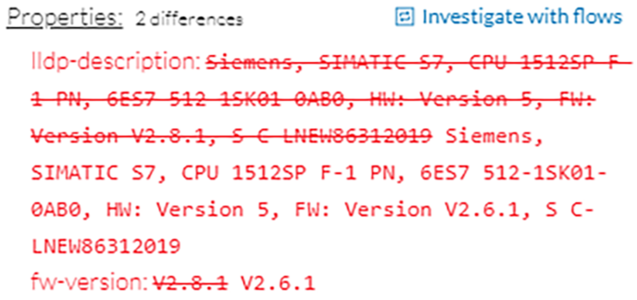
New and changed differences

When a difference is detected, it appears in red in the Monitor mode. There are two types of differences: new and changed ones. A component, an activity, a tag, a property and a variable access can appear (new) or evolve (change). Here below are a few examples of how differences are represented in the Monitor mode:

A new component (plain red) and a changed component (hyphenated red)



Changed component's properties, with the former crossed out property:

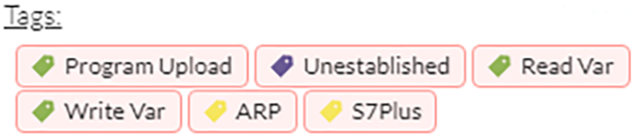


Properties: 2 differences Investigate with flows

lldp-description: ~~Siemens, SIMATIC S7, CPU 1512SP F-1 PN, 6ES7 512-1SK01-0AB0, HW: Version 5, FW: Version V2.8.1, S C-LNEW86312019~~ Siemens, SIMATIC S7, CPU 1512SP F-1 PN, 6ES7 512-1SK01-0AB0, HW: Version 5, FW: Version V2.6.1, S C-LNEW86312019

fw-version: ~~V2.8.1~~ V2.6.1

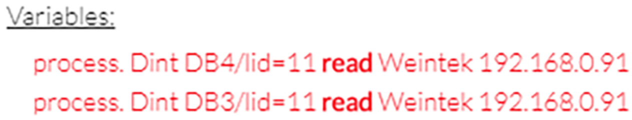
New and changed component and activity tags:



Tags:

Program Upload | Unestablished | Read Var | Write Var | ARP | S7Plus

New and changed activity's variable access:



Variables:

process. Dint DB4/lid=11 **read** Weintek 192.168.0.91

process. Dint DB3/lid=11 **read** Weintek 192.168.0.91

Each difference must be reviewed to identify a potential threat and refine the baseline. Refer to the section Review differences.

Review differences

When differences are detected by the Monitor mode, what one wants to do is to review them to see if they are a potential threat to the network, and clear their data from any red-alarming elements. Several actions are available to help you do so, which will, moreover, allows you to enrich the current baseline, clean it, or report abnormalities. These are available at different levels depending on whether you want to perform a deep behavior review on a component or activity particulars, or at a higher macro level for a quick review. Thus, you can perform these actions on tags, properties, variable accesses, components, activities and baselines.

In any case, any action taken on the Monitor mode will generate an event that you can see on the Events page.

Acknowledge differences

Acknowledge in the Monitor mode

"Acknowledge" is an action to be used to indicate that determined behaviors -or differences- are safe and normal. In fact, by doing this action, the difference will be included in the baseline. You can acknowledge differences on any element of the Monitor mode: tags, properties, variable accesses, components, activities and baselines.

Acknowledge a component or an activity

Acknowledge will display as such if the behavior is notified as changed. However, if the behavior concerning a component or an activity is notified as new, an additional action is required when clicking the button "Acknowledge" because a distinction has to be made according to whether the behavior in question is exceptional or part of an iterative process.

- **Acknowledge & Include**

  This action is to be used for a behavior which is part of a normal process and is meant to happen regularly over time. By using this button, the behavior will be included into the current baseline. If later the component or the activity changes -because for example a new tag has been detected on them- you will be alerted through the Monitor mode: it will turn to "changed" and appear hyphenated and red. This action is useful to refine a baseline as it evolves over time.

  Ex: You can perform this action on a new machine installed in the network, or a new activity due to a new supported protocol.

- **Acknowledge & Keep Warning**

  This action is to be used when a behavior is punctual and not part of a process. In this case, such behavior must not be considered as abnormal but rather as an unusual one, which doesn't have a bad impact on the network. By using this button, the behavior will be acknowledged and so cleared, but will not be included into the baseline. Consequently, you'll be notified if it happens again as a new behavior in the monitored baseline.

  Ex: You can perform this action on a new component and a new activity due to an exceptional maintenance act.

Report differences

This action is to be applied on a difference you consider to be an anomaly, that is, a behavior that is abnormal and may compromise the operating capability and security of the network. However, before reporting the anomaly, the first thing to do is to investigate, and, if possible, to resolve it. In any case, when reporting an anomaly, you must fill in a message of incident response or acknowledgment (in which context the incident has happened, potential threats, or how it has been fixed). Once an anomaly is reported, it is cleared and not included in the baseline, and an event is generated with a default severity level higher than the acknowledge action. You will be alerted in the Monitor mode if the incident occurs again.

Remove and keep warning

This action will remove the component or activity from the current baseline. This is to be used when you consider an element should not appear in a baseline, or you don't want to see it anymore. However, you will be alerted if the component or activity comes back, and the difference will appear as new. This action is also available on variable accesses through Individual acknowledgment.

Note If a difference keeps coming back in a baseline and you don't want to see it, you should modify the preset instead.

Individual acknowledgment

Individual acknowledgment is an advanced usage of Cisco Cyber Vision. This feature is available on changed components and activities, that is, on elements already included in a baseline. It allows you to access their details to perform a deep behavior review by Acknowledge differences and Remove and keep warning one by one the differences detected on the network. Thus, individual acknowledgment is available on components' properties and tags, and on activities' tags and variable accesses.

- **Component properties**

  New and changed properties display in red. Concerning changed properties, the former one is crossed out and the new one displays next to it. They will always display in red, unless you acknowledge them.

- **Component and activity tags**

  New and changed tags display in red. They will be cleared as you acknowledge or report them (i.e. they are no longer displayed in red).

- **Activity variable accesses**

  New and changed variable accesses display in red. A variable access can be acknowledged, reported, and, in addition to other elements, deleted (i.e. button "**Remove and keep warning**"). Deleting a variable access is to be used when you consider that it should not be part of the current baseline and you don't want to see it. It will be removed from the baseline and disappear. If, however, the variable access happens again, you will be alerted and it will display in red.

Once all component or activity's elements are reviewed (i.e. acknowledged, reported, or removed), the entity they belong to is cleared (the component or activity itself is no longer displayed in red). Any action performed in the Monitor mode will appear in the Event page.

Investigate with flows

This button is not an action but an option to get more information and context about the differences detected on the network. In fact, each difference found, since it belongs to a component or an activity, is related to a flow. This view allows you to perform forensic analysis and may give you some clues to understand what happened.

Ex: You can search from which flow exactly a tag comes from.

Create a baseline from a default preset

1. Access the Explore page.
2. In Basics, click the preset Essential data.
3. Click the button Add a new baseline from preset.

4. A pop-up appears to invite you to check your new baseline. Click Go check it out.
5. All elements displays. Some components and activities may already appear in red as new or changed.

Create a baseline from a group

To create groups:

Procedure

Step 1 Access the All data preset.

Step 2 Create two groups of components.

Step 3 Click the Autolayout button.

Example:

We create a group HMI and a group PLC.

To create presets from groups:

Step 4 In criteria, access the groups filter, and select the first one of the group you created.

Example:

We select the HMI group in the filter.

The HMI group displays in the map with its related activities.

Step 5 Create a preset from this view.

Step 6 Click Save as and name the preset HMI.

Step 7 Repeat the previous steps for the PLC group.

Step 8 Go to All Presets. You will see your two new presets.

To create a baseline from presets:

Step 9 Access the HMI preset.

Step 10 Click the button "Add a new baseline from preset".

Step 11 Name it HMI.

Step 12 Repeat the previous steps for the PLC preset.

Step 13 Access the Monitor mode. You will see your two new baselines.

Create a weekend baseline

Create another baseline to monitor the network during weekends.

1. Access the All data preset.
2. Set the period for the weekend. For example, from Friday 5 p.m. to Monday 4 a.m.

3. Click the button "Add a new baseline from preset".
4. Name the baseline "All data weekend" and add the description "Must be active from Friday 5pm till Monday 4am".

Enable a baseline monitoring

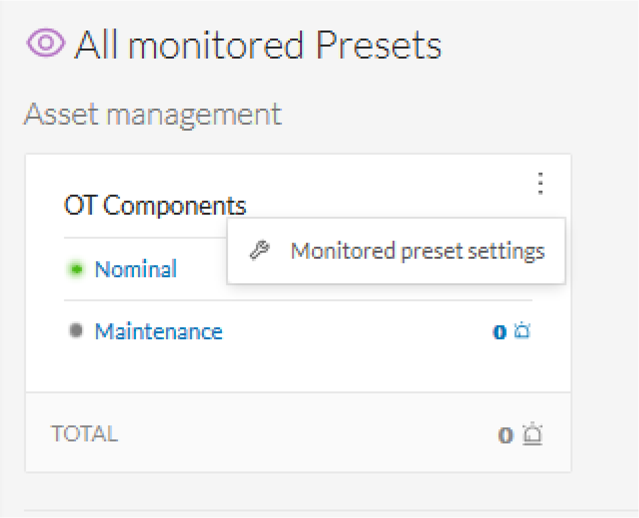
To make the most of the Monitor mode, it is sometimes insightful to create several baselines per preset. However, only one baseline can be active at a time per preset. This is because a baseline is to be used to monitor a well-defined network process during a specific period of time (e.g. baselines Normal operating mode, Maintenance, Week-end, Night). Two baselines cannot happen at the same time on a preset, and you need to enable the proper baseline as the network enters a new operating phase. Consequently, when you enable a baseline on a preset, the active one is automatically disabled.

To enable a baseline:

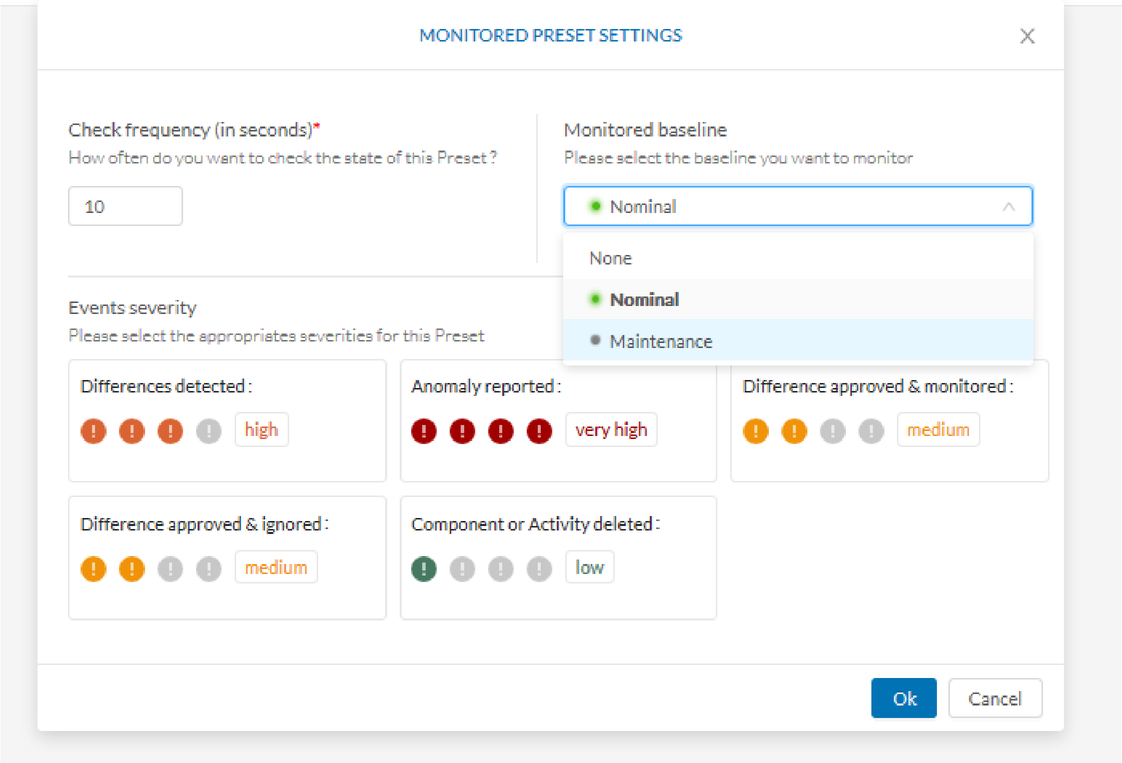
Procedure

Step 1 Access the Monitor page.

Step 2 Click the monitored preset settings menu on the preset you want to monitor.



Step 3 Under Monitored baseline, select the baseline you want to enable.



MONITORED PRESET SETTINGS

Check frequency (in seconds)*
How often do you want to check the state of this Preset ?

10

Monitored baseline
Please select the baseline you want to monitor

● Nominal

None
● Nominal
● Maintenance

Events severity
Please select the appropriates severities for this Preset

Differences detected : high

Anomaly reported : very high

Difference approved & monitored : medium

Difference approved & ignored : medium

Component or Activity deleted : low

Step 4 Click Ok.

The baseline selected turns to green and is enabled.

Use cases

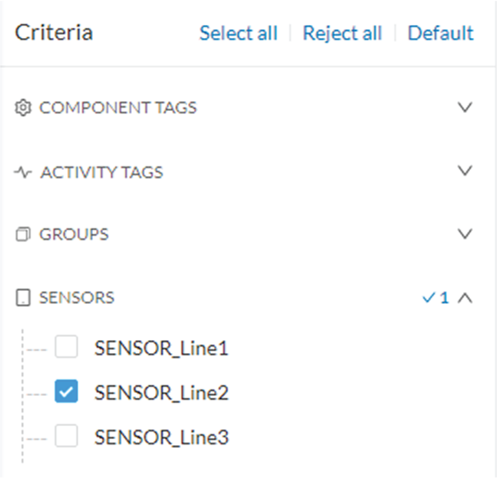
Detection of assets newly connected to the network

A basic use case in Cisco Cyber Vision is to detect if and when a new equipment connects to the industrial network being monitored. However, the first thing to do when using Cisco Cyber Vision is to organize components in an intelligible way. In this use case, we choose to organize components according to the network's topology, that is, per production chain. In fact, a network can be divided into several areas, such as several production chains with different criticality levels, where a Cisco Cyber Vision Sensor is placed to capture and monitor its traffic. This topology can be reflected in Cisco Cyber Vision by creating groups which represent a production chain and contain its components. In clear, here we intend to detect a new component and its related activities within a specific area. Thus, it will be possible to see whether a component connects with this production chain. Its related activities will also be highlighted in the Monitor mode.

Key Differences: New components and their related activities on the network

Aim: Monitor the production line 2 of the industrial network.

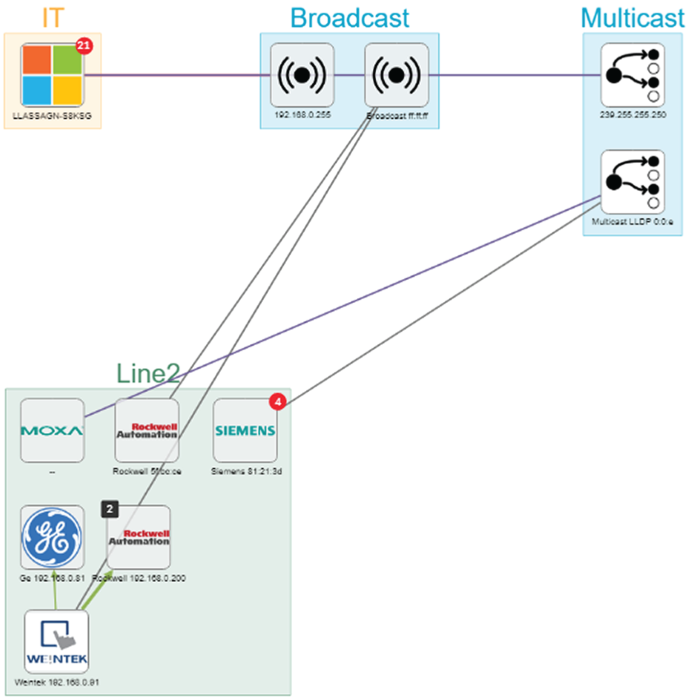
Since a sensor is placed on each production chain, we use the sensor filter to display each production chain. In our example, the industrial network we're monitoring has 3 production lines on which we have positioned a sensor. We want to see and monitor what is happening on production line 2. To do so, we access the Preset All data in the Explore mode and we select the filter SENSOR_Line2 (it is possible to rename sensors to identify which area of the network they're monitoring) so only traffic captured on Production Line 2 appears.


Criteria

□ SENSOR_Line1
☑ SENSOR_Line2
□ SENSOR_Line3

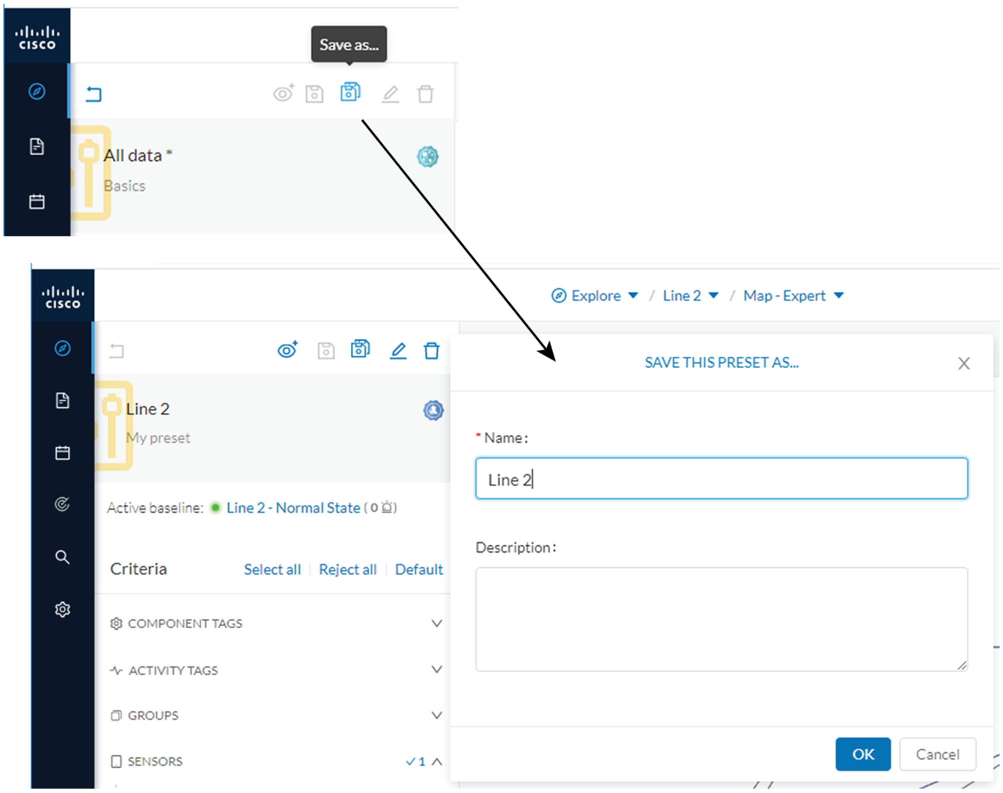
What we need to do then, is to organize the components into groups, per function:

- PLCs in Line 2
- IT
- Broadcast
- Multicast



As a result, we have a filtered and organized view of production chain 2.

Now that the network data is filtered and grouped, we save the selection as a new preset that we name Line 2.



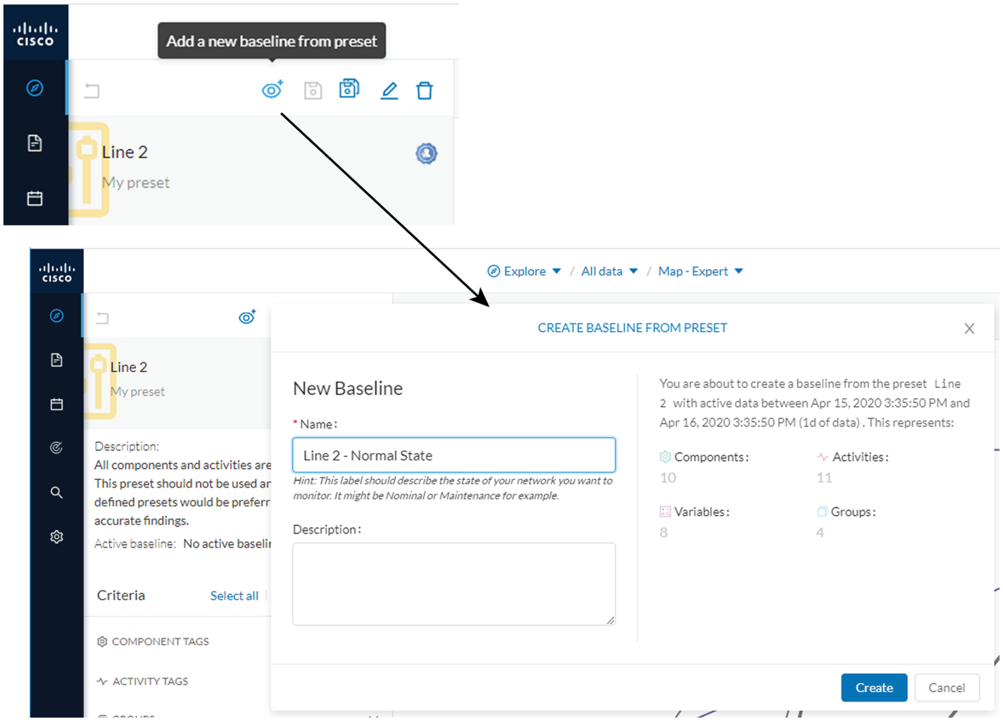
Active baseline: ● Line 2 - Normal State (0)

SAVE THIS PRESET AS...

* Name: Line 2

Description:

The preset Line 2 contains components and activities we consider to be interacting in a normal way, that is, production line 2 is in normal operating state. We save the preset's normal state as a baseline that we name Line 2 - Normal State.



Description:
All components and activities are
This preset should not be used ar
defined presets would be preferr
accurate findings.
Active baseline: No active baselir

New Baseline

* Name: Line 2 - Normal State

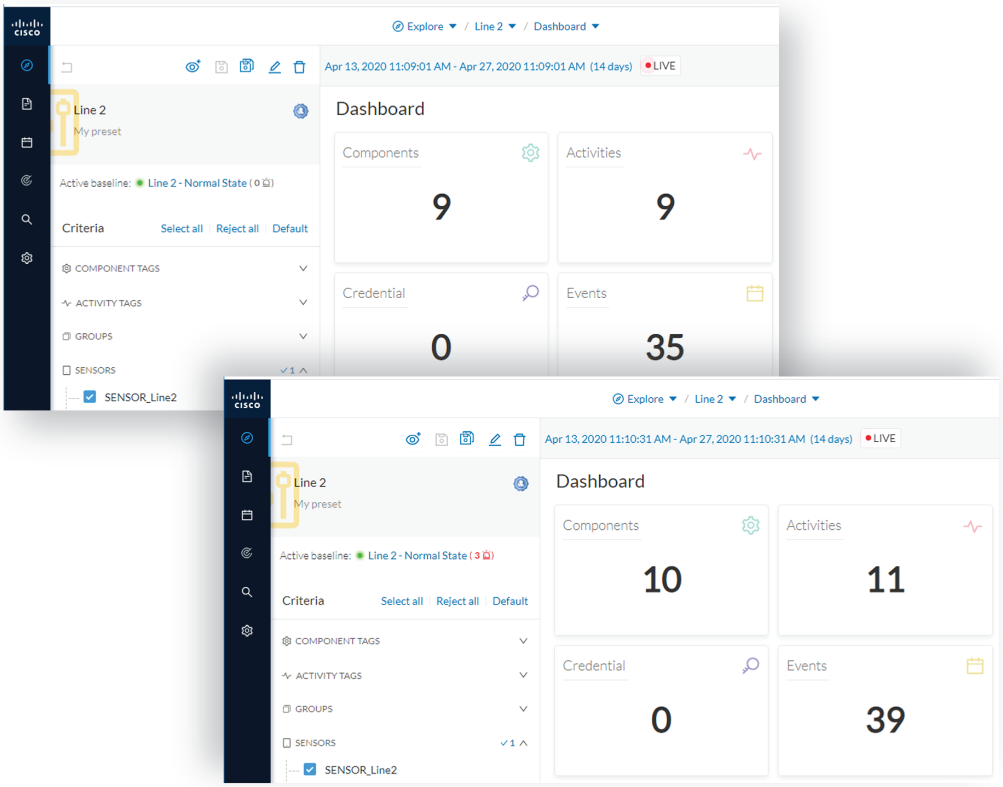
Hint: This label should describe the state of your network you want to monitor. It might be Nominal or Maintenance for example.

Description:

You are about to create a baseline from the preset Line 2 with active data between Apr 15, 2020 3:35:50 PM and Apr 16, 2020 3:35:50 PM (1d of data) . This represents:

Components: 10
Activities: 11
Variables: 8
Groups: 4

We come back later to check Production Line 2. As we access the Explore mode we notice that there are 10 components instead of 9. Number of activities and events have increased too. The baseline Line 2 - Normal State reports 3 alerts.

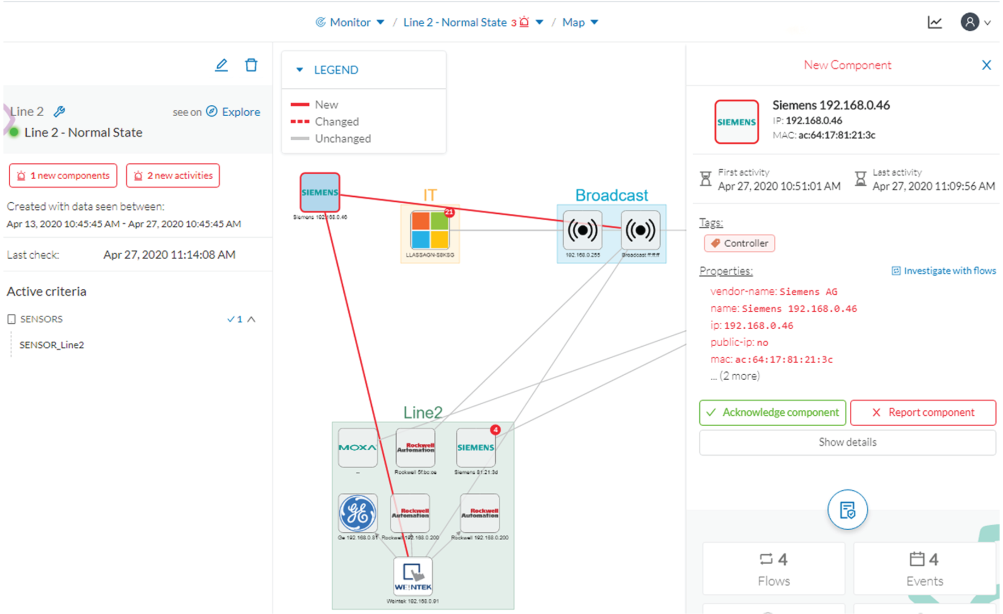


To understand what had happened exactly, we access the baseline in the Monitor mode.

The left panel indicates that 1 new component and 2 new activities have been found.

As we click the new component, the right side panel opens with the component's detailed properties.

As we observe the component's details, we learn that it is in fact a controller, and properties look like what we're already used to see on the network regarding other components' characteristics. After confirming on site, we discover that a new PLC has been connected to the network to enlarge Production Line 2.



Line 2
Line 2 - Normal State

1 new components
2 new activities

Created with data seen between:
Apr 13, 2020 10:45:45 AM - Apr 27, 2020 10:45:45 AM

Last check: Apr 27, 2020 11:14:08 AM

Active criteria

□ SENSORS ✓1

SENSOR_Line2

New Component

Siemens 192.168.0.46
IP: 192.168.0.46
MAC: ac:64:17:81:21:3c

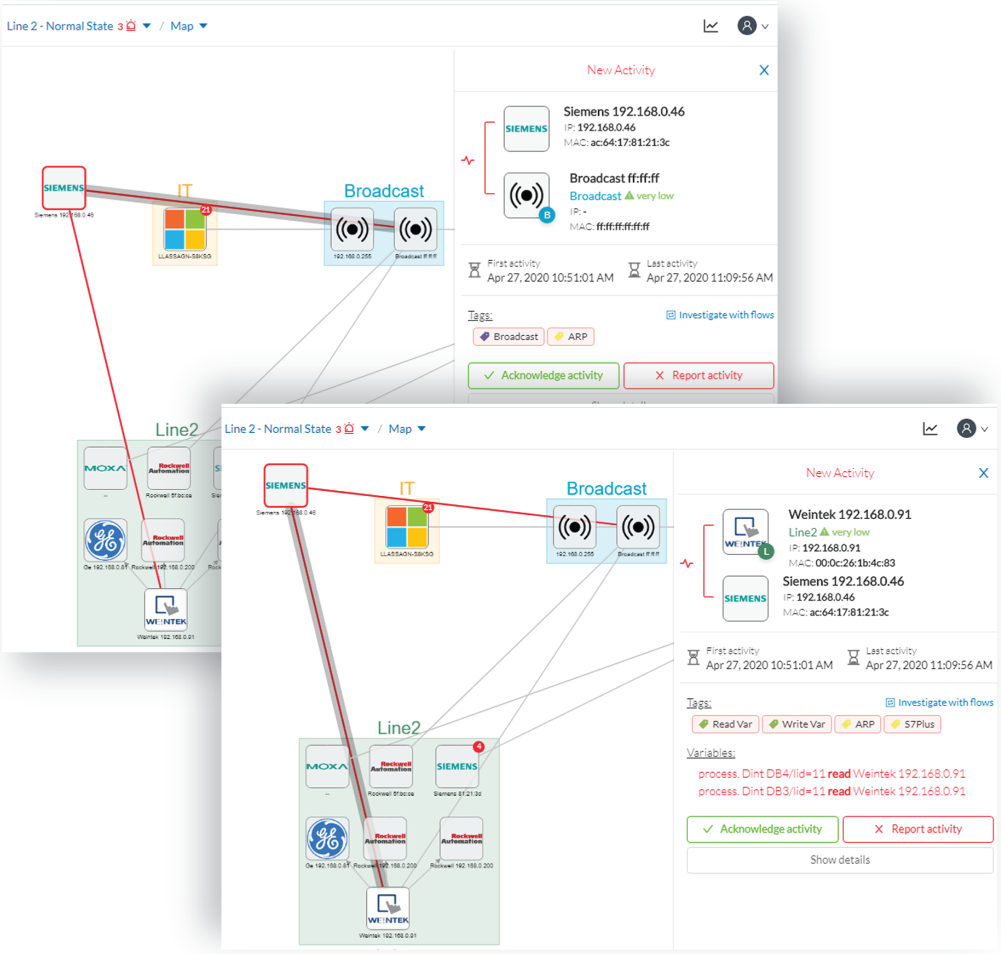
First activity Apr 27, 2020 10:51:01 AM
Last activity Apr 27, 2020 11:09:56 AM

Tags:
Controller

Properties:
vendor-name: Siemens AG
name: Siemens 192.168.0.46
ip: 192.168.0.46
public-ip: no
mac: ac:64:17:81:21:3c
... (2 more)

4 Flows
4 Events

Then, we check that this new component behaves normally by looking at its activities. It has been identified because it has sent a broadcast packet (probably ARP) and then has connected to the Weintek machine using a legitimate protocol. Actions like Read variable accesses look normal too.



New Activity

Siemens 192.168.0.46
IP: 192.168.0.46
MAC: ac:64:17:81:21:3c

Broadcast ff:ff:ff
Broadcast very low
IP: -
MAC: ff:ff:ff:ff:ff:ff

First activity Apr 27, 2020 10:51:01 AM
Last activity Apr 27, 2020 11:09:56 AM

Tags: Broadcast, ARP
Investigate with flows

✓ Acknowledge activity
X Report activity

New Activity

Weintek 192.168.0.91
Line2 very low
IP: 192.168.0.91
MAC: 00:0c:26:1b:4c:83

Siemens 192.168.0.46
IP: 192.168.0.46
MAC: ac:64:17:81:21:3c

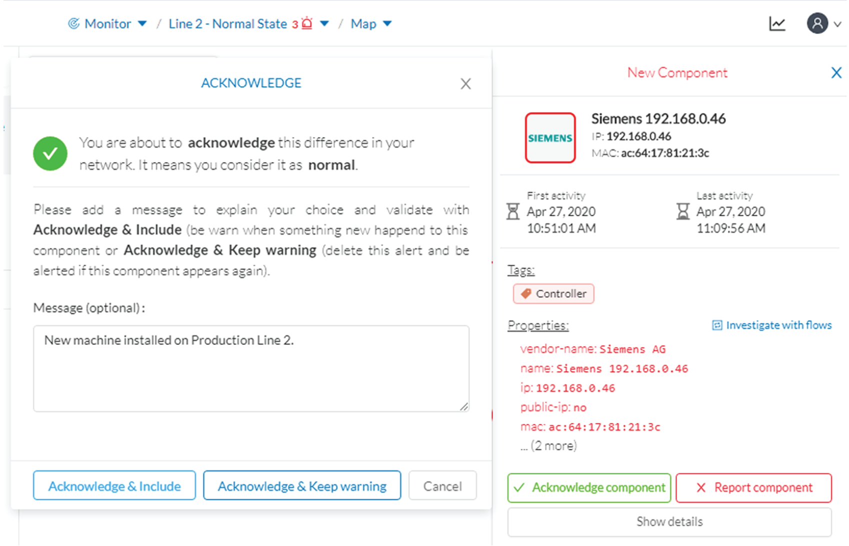
First activity Apr 27, 2020 10:51:01 AM
Last activity Apr 27, 2020 11:09:56 AM

Tags: Read Var, Write Var, ARP, S7Plus
Investigate with flows

Variables:
process. Dint DB4/lid=11 **read** Weintek 192.168.0.91
process. Dint DB3/lid=11 **read** Weintek 192.168.0.91

✓ Acknowledge activity
X Report activity
Show details

Since the component and activities will be part of the normal operating process of Production Line 2, the differences can be acknowledged and included in the baseline to be notified if any change occurs.



You are about to **acknowledge** this difference in your network. It means you consider it as **normal**.

Please add a message to explain your choice and validate with **Acknowledge & Include** (be warn when something new happend to this component or **Acknowledge & Keep warning** (delete this alert and be alerted if this component appears again).

Message (optional) :

New machine installed on Production Line 2.

Siemens 192.168.0.46
IP: 192.168.0.46
MAC: ac:64:17:81:21:3c

First activity Apr 27, 2020 10:51:01 AM
Last activity Apr 27, 2020 11:09:56 AM

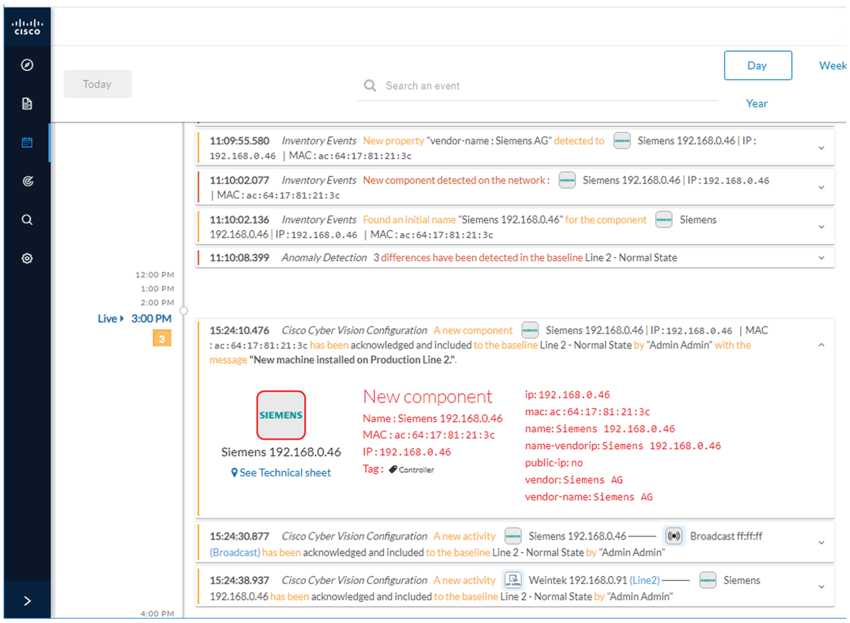
Tags:
Controller

Properties:

vendor-name: Siemens AG
name: Siemens 192.168.0.46
ip: 192.168.0.46
public-ip: no
mac: ac:64:17:81:21:3c
... (2 more)

We return to the Explore mode and add the component into the Line 2 group.

Eventually, we access the Events page and see that all previous actions are reported here, from the detection of a new component and activities on the network, to adding the component into the group Line 2.



11:09:55.580 *Inventory Events* New property "vendor-name : Siemens AG" detected to Siemens 192.168.0.46 | IP : 192.168.0.46 | MAC : ac:64:17:81:21:3c

11:10:02.077 *Inventory Events* New component detected on the network : Siemens 192.168.0.46 | IP : 192.168.0.46 | MAC : ac:64:17:81:21:3c

11:10:02.136 *Inventory Events* Found an initial name "Siemens 192.168.0.46" for the component Siemens 192.168.0.46 | IP : 192.168.0.46 | MAC : ac:64:17:81:21:3c

11:10:08.399 *Anomaly Detection* 3 differences have been detected in the baseline Line 2 - Normal State

15:24:10.476 *Cisco Cyber Vision Configuration* A new component Siemens 192.168.0.46 | IP : 192.168.0.46 | MAC : ac:64:17:81:21:3c has been acknowledged and included to the baseline Line 2 - Normal State by "Admin Admin" with the message "New machine installed on Production Line 2.".

Siemens 192.168.0.46
See Technical sheet

New component
Name : Siemens 192.168.0.46
MAC : ac:64:17:81:21:3c
IP : 192.168.0.46
Tag : Controller

ip: 192.168.0.46
mac: ac:64:17:81:21:3c
name: Siemens 192.168.0.46
name-vendorip: Siemens 192.168.0.46
public-ip: no
vendor: Siemens AG
vendor-name: Siemens AG

15:24:30.877 *Cisco Cyber Vision Configuration* A new activity Siemens 192.168.0.46 —— Broadcast ff:ff:ff (Broadcast) has been acknowledged and included to the baseline Line 2 - Normal State by "Admin Admin"

15:24:38.937 *Cisco Cyber Vision Configuration* A new activity Weintek 192.168.0.91 (Line2) —— Siemens 192.168.0.46 has been acknowledged and included to the baseline Line 2 - Normal State by "Admin Admin"

Tracking sensitive assets properties

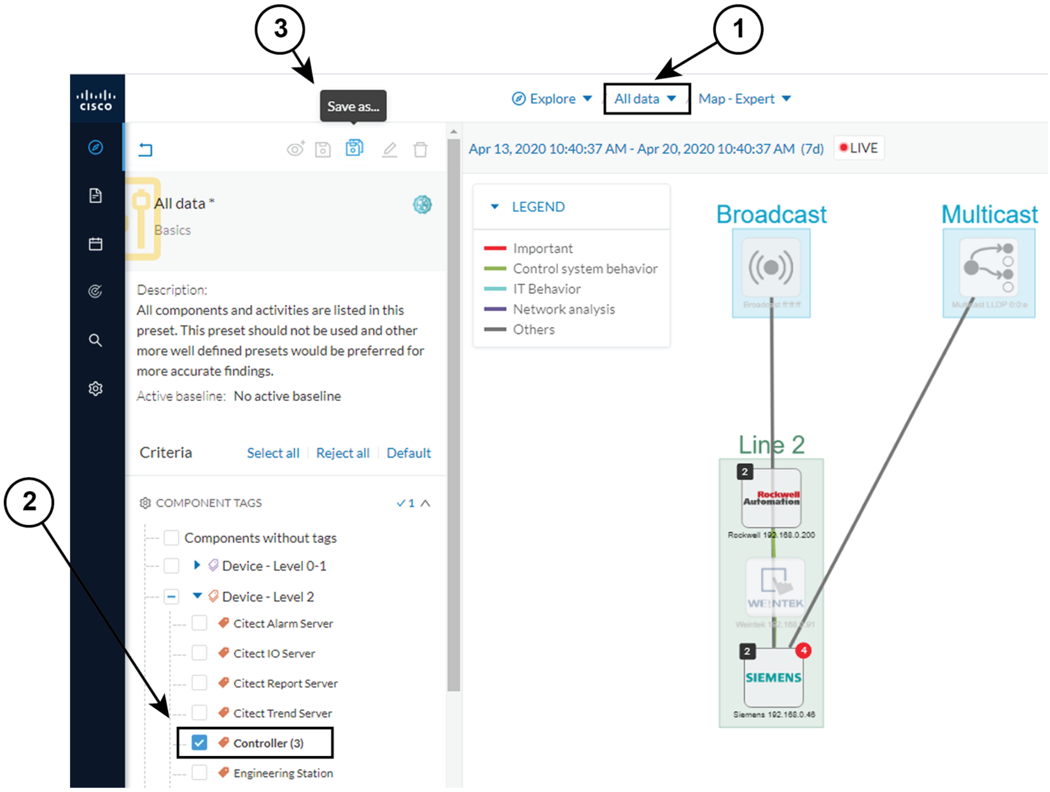
To ensure a network's security, its critical assets need to be monitored closely. Usually, critical assets are controllers which ensure the plant's operation. To monitor them, we're going to check its properties. The properties to keep an eye on are programs and firmware versions changes that might cause malfunctions or even stop a production line.

Preset Definition: Preset need to be defined per Group or multiple Group

Key Differences: New properties or changed properties on components

In the Explore mode, we access the Preset All data (1). We group the components per function (Broadcast, Multicast, Production Line 2) to organize our data. We select the Controllers component filter (2), so only the components marked with the Controller tag, their activities and related components display.

Now that the network data is filtered and grouped, we save the selection as a new preset (3) that we name Controllers.

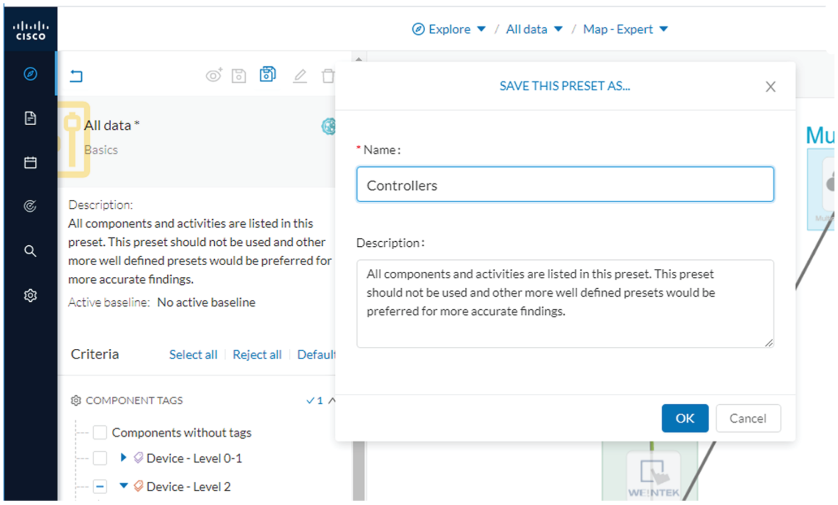


Apr 13, 2020 10:40:37 AM - Apr 20, 2020 10:40:37 AM (7d) ●LIVE

Description:
All components and activities are listed in this preset. This preset should not be used and other more well defined presets would be preferred for more accurate findings.

Active baseline: No active baseline

- □ Components without tags
- □ ▸ Device - Level 0-1
- ⊟ ▾ Device - Level 2
  - □ Citect Alarm Server
  - □ Citect IO Server
  - □ Citect Report Server
  - □ Citect Trend Server
  - ☑ Controller (3)
  - □ Engineering Station



SAVE THIS PRESET AS...

* Name: Controllers

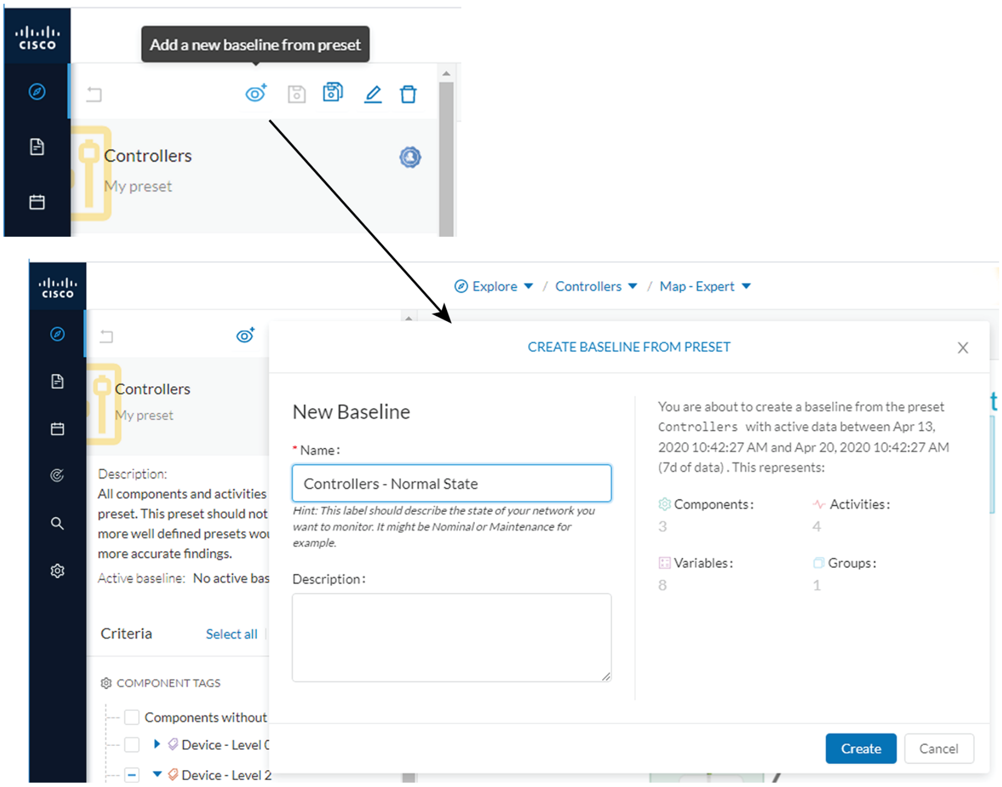
Description: All components and activities are listed in this preset. This preset should not be used and other more well defined presets would be preferred for more accurate findings.

OK Cancel

Description: All components and activities are listed in this preset. This preset should not be used and other more well defined presets would be preferred for more accurate findings.

Active baseline: No active baseline

The preset Controllers contains components and activities we consider to be operating in a normal way. We save the preset's normal state as a baseline that we name Controllers - Normal State.



CREATE BASELINE FROM PRESET

New Baseline

* Name: Controllers - Normal State

Hint: This label should describe the state of your network you want to monitor. It might be Nominal or Maintenance for example.

Description:

You are about to create a baseline from the preset `Controllers` with active data between Apr 13, 2020 10:42:27 AM and Apr 20, 2020 10:42:27 AM (7d of data). This represents:

Components: 3

Activities: 4

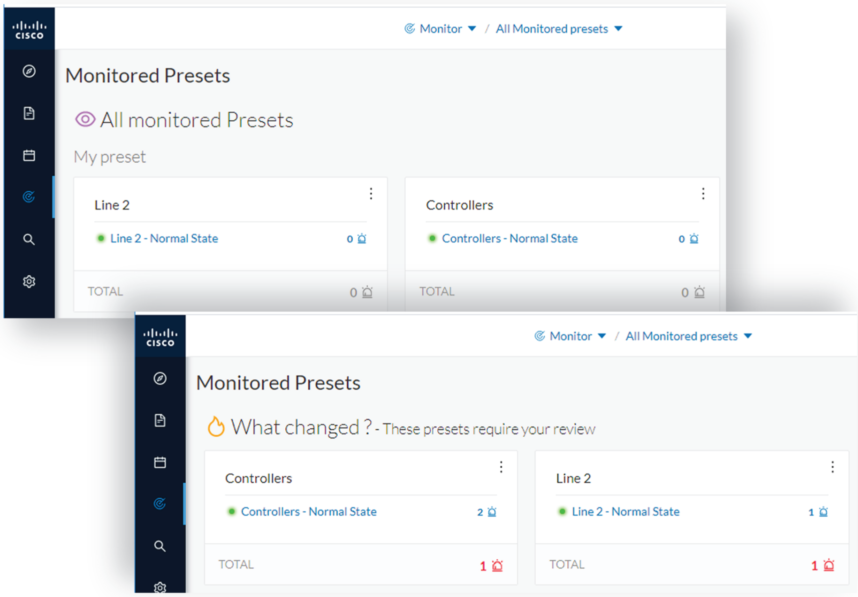
Variables: 8

Groups: 1

Create Cancel

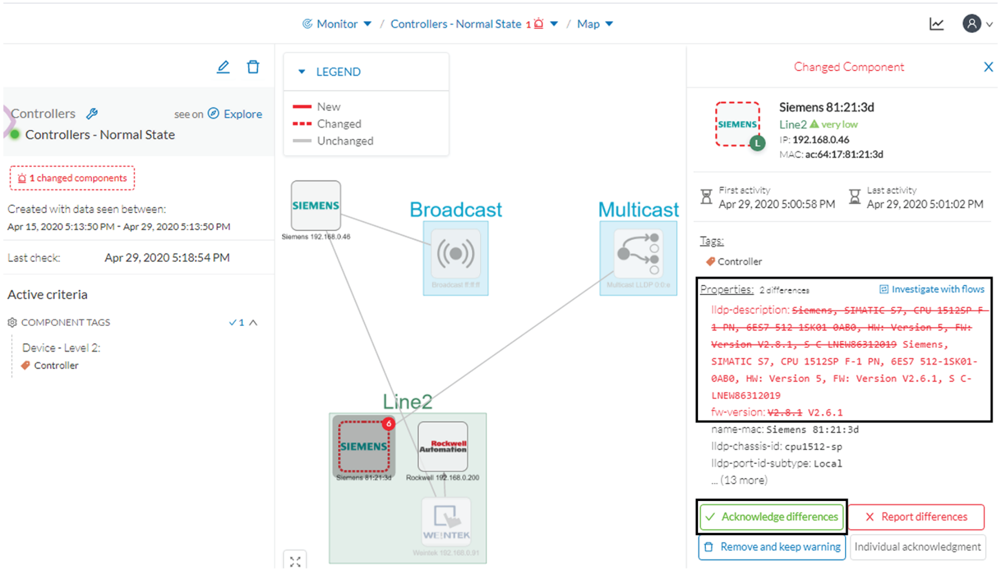
We access the Monitor mode. The new baseline Controllers - Normal State displays.

A few moments pass and two alerts are reported in the Controllers preset. We access the baseline to see what happened.



The left panel reports that one component and one activity have changed in the scope of the preset.

As we click on the changed component in the map, a right side panel opens with more information. Changes appear in red. The tag indicates that it's a controller. The properties lldp-description and firmware version have changed and the former version is crossed off.



Created with data seen between:
Apr 15, 2020 5:13:50 PM - Apr 29, 2020 5:13:50 PM

Last check: Apr 29, 2020 5:18:54 PM

Active criteria

COMPONENT TAGS ✓1

Device - Level 2:
Controller

Siemens 81:21:3d
Line2 very low
IP: 192.168.0.46
MAC: ac:64:17:81:21:3d

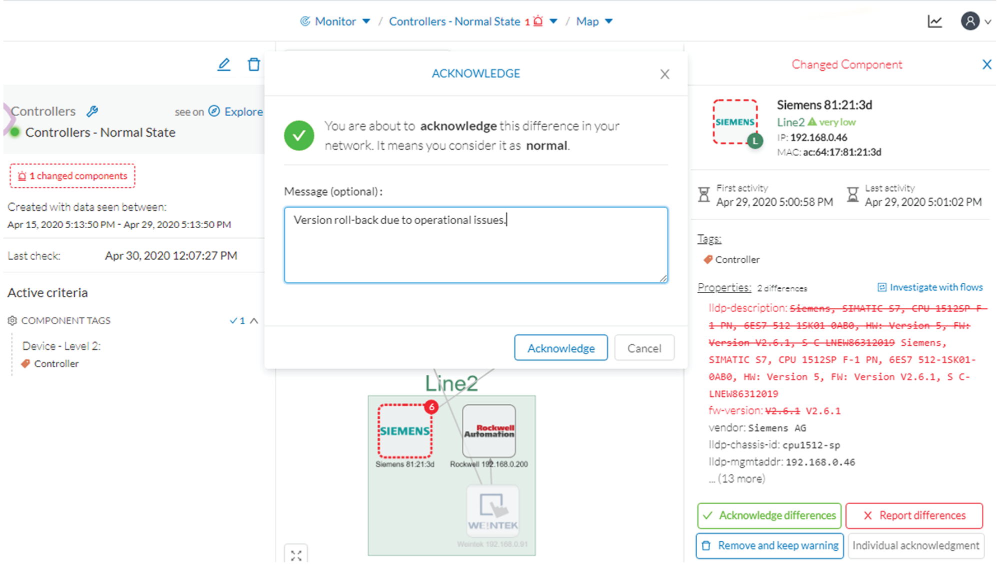
First activity Apr 29, 2020 5:00:58 PM
Last activity Apr 29, 2020 5:01:02 PM

Tags:
Controller

Properties: 2 differences

lldp-description: ~~Siemens, SIMATIC S7, CPU 1512SP F-1 PN, 6ES7 512-1SK01-0AB0, HW: Version 5, FW: Version V2.8.1, S C-LNEW86312019~~ Siemens, SIMATIC S7, CPU 1512SP F-1 PN, 6ES7 512-1SK01-0AB0, HW: Version 5, FW: Version V2.6.1, S C-LNEW86312019
fw-version: ~~V2.8.1~~ V2.6.1
name-mac: Siemens 81:21:3d
lldp-chassis-id: cpu1512-sp
lldp-port-id-subtype: Local
... (13 more)

The particularity here is that no activity on the network seems to explain why the SIEMENS component's firmware version rolled back. To figure this out, we meet with the technical operator in charge of the production line. This person informs us that the latest version was causing several issues on the network. Consequently, a rollback has been performed by a maintenance operator to solve these until a new fix comes out. We conclude that this was part of a normal maintenance act and we acknowledge the differences.



Created with data seen between:
Apr 15, 2020 5:13:50 PM - Apr 29, 2020 5:13:50 PM

Last check: Apr 30, 2020 12:07:27 PM

ACKNOWLEDGE

You are about to **acknowledge** this difference in your network. It means you consider it as **normal**.

Message (optional): Version roll-back due to operational issues.

Acknowledge Cancel

Siemens 81:21:3d
Line2 very low
IP: 192.168.0.46
MAC: ac:64:17:81:21:3d

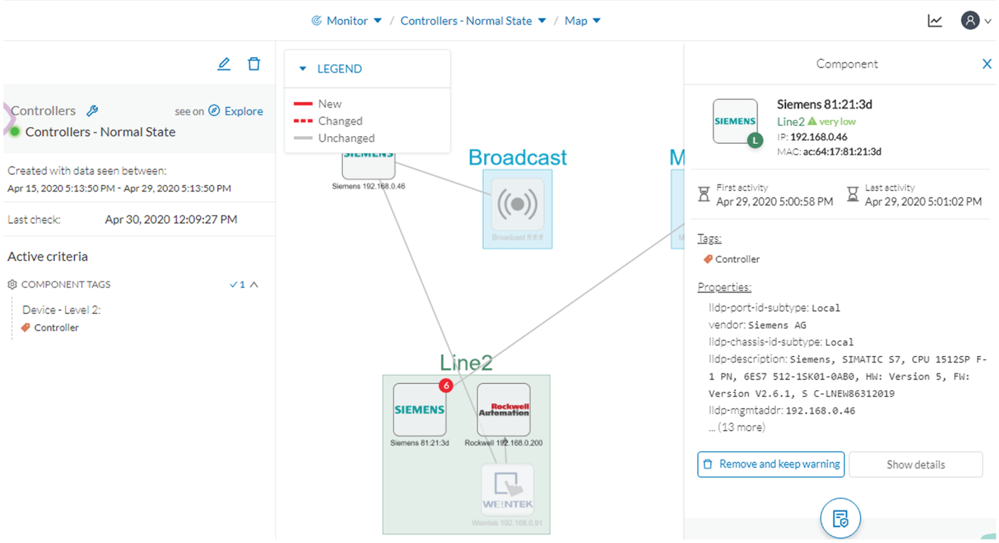
First activity Apr 29, 2020 5:00:58 PM
Last activity Apr 29, 2020 5:01:02 PM

Tags:
Controller

Properties: 2 differences

lldp-description: ~~Siemens, SIMATIC S7, CPU 1512SP F-1 PN, 6ES7 512 1SK01 0AB0, HW: Version 5, FW: Version V2.6.1, S C LNEW86312019~~ Siemens, SIMATIC S7, CPU 1512SP F-1 PN, 6ES7 512-1SK01-0AB0, HW: Version 5, FW: Version V2.6.1, S C-LNEW86312019
fw-version: ~~V2.6.1~~ V2.6.1
vendor: Siemens AG
lldp-chassis-id: cpu1512-sp
lldp-mgmtaddr: 192.168.0.46
... (13 more)

Once differences are acknowledged, they are considered as normal and do not appear in red anymore. If a new change happens such as the version update, the component will appear as changed again in the Monitor mode.



Created with data seen between:
Apr 15, 2020 5:13:50 PM - Apr 29, 2020 5:13:50 PM

Last check: Apr 30, 2020 12:09:27 PM

Siemens 81:21:3d
Line2 very low
IP: 192.168.0.46
MAC: ac:64:17:81:21:3d

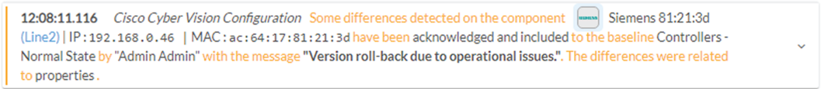
First activity Apr 29, 2020 5:00:58 PM
Last activity Apr 29, 2020 5:01:02 PM

Tags:
Controller

Properties:

lldp-port-id-subtype: Local
vendor: Siemens AG
lldp-chassis-id-subtype: Local
lldp-description: Siemens, SIMATIC S7, CPU 1512SP F-1 PN, 6ES7 512-1SK01-0AB0, HW: Version 5, FW: Version V2.6.1, S C-LNEW86312019
lldp-mgmtaddr: 192.168.0.46
... (13 more)

An event is generated accordingly to the previous behaviors that have happened on preset Controllers and actions.



12:08:11.116 *Cisco Cyber Vision Configuration* Some differences detected on the component Siemens 81:21:3d (Line2) | IP : 192.168.0.46 | MAC : ac:64:17:81:21:3d have been acknowledged and included to the baseline Controllers - Normal State by "Admin Admin" with the message **"Version roll-back due to operational issues."**. The differences were related to properties .

Detect changes that impact availability and integrity

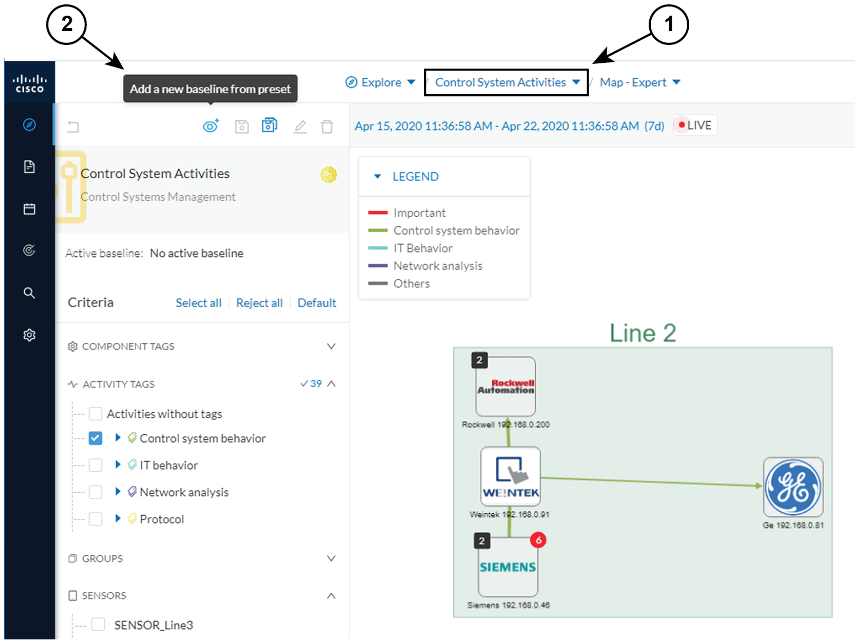
First evidence that someone might have hacked your industrial control system and is trying to disrupt your industrial processes are Stop CPU orders or new programs sent into a Controller's memory. A station that starts to send such content inside a network must be detected as soon as possible. It is possible to monitor a network by watching all control system behaviors.

This can be done in Cisco Cyber Vision by using the Control System Activities preset, which is a default preset and will check all activity tags categorized as Control System Behavior and consequently all related components. Key differences in such use case are new or changed activities. Moreover, components' tags and properties will give further context to help understanding of what is happening in the network.

Preset Definition: Preset need to be defined per activities tag like "Control Systems Behaviors"

Key Differences: New or changed activities

To do so, we access the preset Control System Activities (1) and we create a baseline from this preset (2) that we name Control System Activities - Normal State (3).

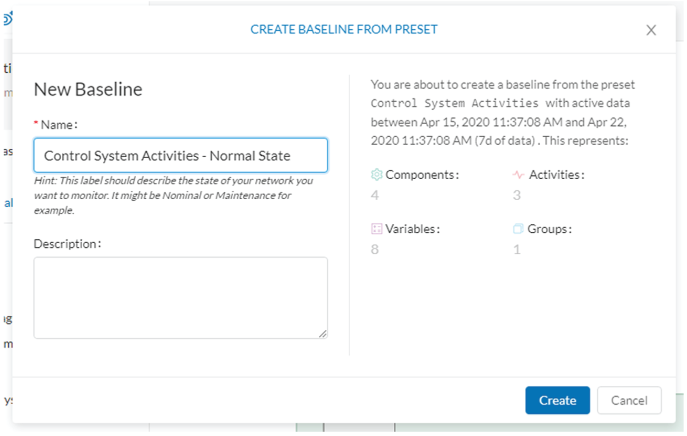


Apr 15, 2020 11:36:58 AM - Apr 22, 2020 11:36:58 AM (7d)

Active baseline: No active baseline

□ Activities without tags
☑ Control system behavior
□ IT behavior
□ Network analysis
□ Protocol

□ SENSOR_Line3



CREATE BASELINE FROM PRESET

New Baseline

* Name:

Control System Activities - Normal State

Hint: This label should describe the state of your network you want to monitor. It might be Nominal or Maintenance for example.

Description:

You are about to create a baseline from the preset `Control System Activities` with active data between Apr 15, 2020 11:37:08 AM and Apr 22, 2020 11:37:08 AM (7d of data). This represents:

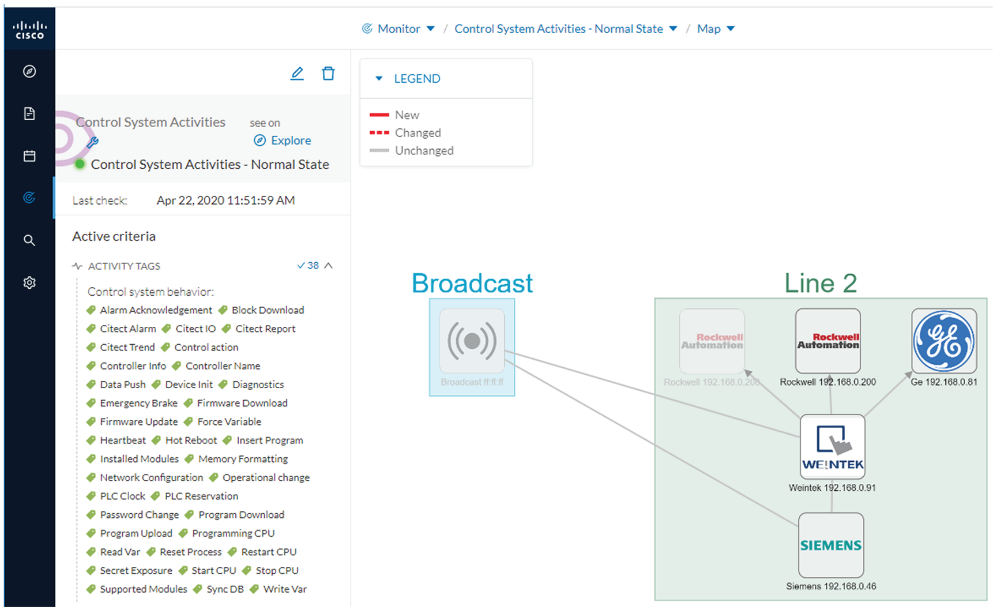
Components: 4

Activities: 3

Variables: 8

Groups: 1

As we access the Monitor mode we can access and see the Control System Activities's baseline we just created. Nothing has happened yet on the preset.



Monitor / Control System Activities - Normal State / Map

Control System Activities

see on Explore

Control System Activities - Normal State

Last check: Apr 22, 2020 11:51:59 AM

Active criteria

ACTIVITY TAGS ✓38

Control system behavior:

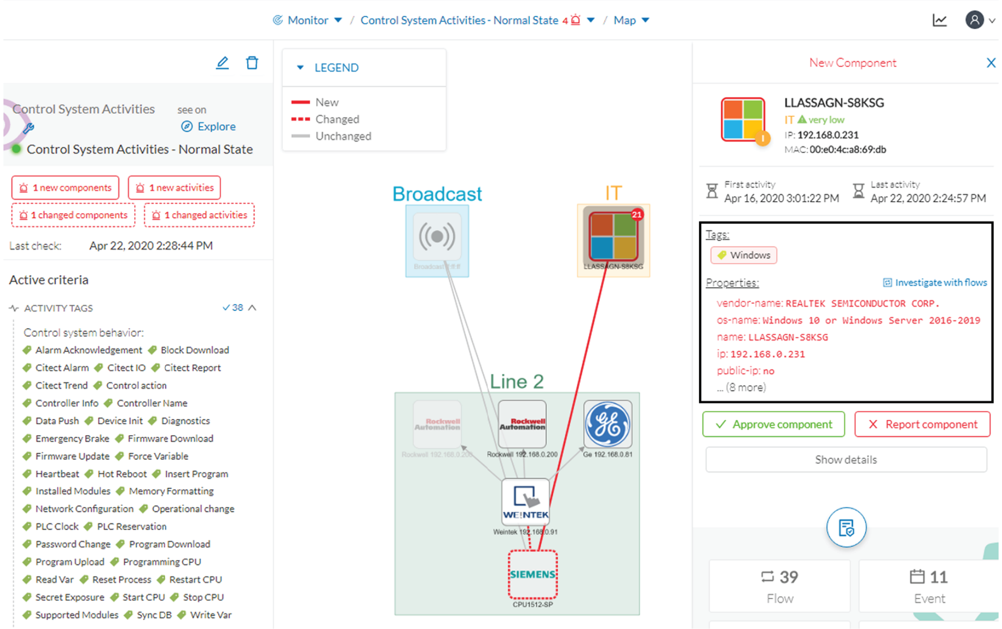
Alarm Acknowledgement, Block Download, Citect Alarm, Citect IO, Citect Report, Citect Trend, Control action, Controller Info, Controller Name, Data Push, Device Init, Diagnostics, Emergency Brake, Firmware Download, Firmware Update, Force Variable, Heartbeat, Hot Reboot, Insert Program, Installed Modules, Memory Formatting, Network Configuration, Operational change, PLC Clock, PLC Reservation, Password Change, Program Download, Program Upload, Programming CPU, Read Var, Reset Process, Restart CPU, Secret Exposure, Start CPU, Stop CPU, Supported Modules, Sync DB, Write Var

LEGEND

- New
- Changed
- Unchanged

After a few moments, new differences are detected on the preset. The left panel and the Map help identifying what has happened: a new component had an activity which changed another component and its activity with another component (1).

Clicking the new component (2) opens a right side panel which offers more information. The tag Windows indicates that the new component is a Windows machine (3). Below, its properties are listed and give more information about the machine.



Control System Activities see on Explore

Control System Activities - Normal State

1 new components | 1 new activities
1 changed components | 1 changed activities

Last check: Apr 22, 2020 2:28:44 PM

Active criteria

ACTIVITY TAGS ✓38

Control system behavior:
Alarm Acknowledgement, Block Download, Citect Alarm, Citect IO, Citect Report, Citect Trend, Control action, Controller Info, Controller Name, Data Push, Device Init, Diagnostics, Emergency Brake, Firmware Download, Firmware Update, Force Variable, Heartbeat, Hot Reboot, Insert Program, Installed Modules, Memory Formatting, Network Configuration, Operational change, PLC Clock, PLC Reservation, Password Change, Program Download, Program Upload, Programming CPU, Read Var, Reset Process, Restart CPU, Secret Exposure, Start CPU, Stop CPU, Supported Modules, Sync DB, Write Var

New Component

LLASSAGN-S8KSG
IT very low
IP: 192.168.0.231
MAC: 00:e0:4c:a8:69:db

First activity Apr 16, 2020 3:01:22 PM
Last activity Apr 22, 2020 2:24:57 PM

Tags:
Windows

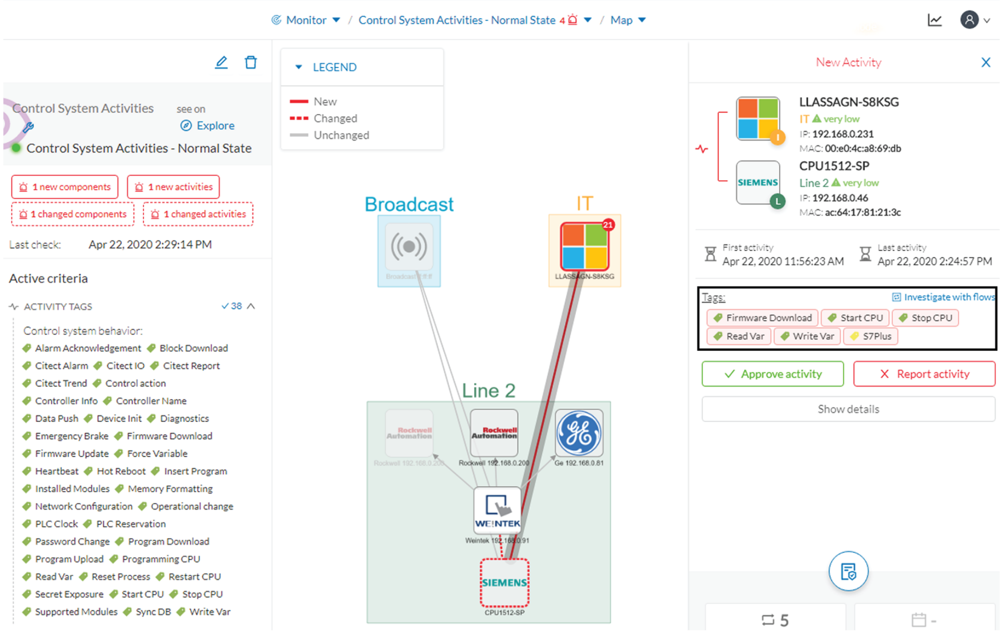
Properties: Investigate with flows
vendor-name: REALTEK SEMICONDUCTOR CORP.
os-name: Windows 10 or Windows Server 2016-2019
name: LLASSAGN-S8KSG
ip: 192.168.0.231
public-ip: no
... (8 more)

✓ Approve component | X Report component

Show details

39 Flow | 11 Event

Clicking the new activity between the new machine and the CPU opens its right side panel and gives more information about what happened. New tags such as Firmware Download, Start CPU, Stop CPU, Read and Write Var, which are suspicious, indicate the type of actions the new Windows machine has performed on the CPU.



Control System Activities see on Explore

Control System Activities - Normal State

1 new components | 1 new activities
1 changed components | 1 changed activities

Last check: Apr 22, 2020 2:29:14 PM

Active criteria

ACTIVITY TAGS ✓38

Control system behavior:
Alarm Acknowledgement, Block Download, Citect Alarm, Citect IO, Citect Report, Citect Trend, Control action, Controller Info, Controller Name, Data Push, Device Init, Diagnostics, Emergency Brake, Firmware Download, Firmware Update, Force Variable, Heartbeat, Hot Reboot, Insert Program, Installed Modules, Memory Formatting, Network Configuration, Operational change, PLC Clock, PLC Reservation, Password Change, Program Download, Program Upload, Programming CPU, Read Var, Reset Process, Restart CPU, Secret Exposure, Start CPU, Stop CPU, Supported Modules, Sync DB, Write Var

New Activity

LLASSAGN-S8KSG
IT very low
IP: 192.168.0.231
MAC: 00:e0:4c:a8:69:db

CPU1512-SP
Line 2 very low
IP: 192.168.0.46
MAC: ac:64:17:81:21:3c

First activity Apr 22, 2020 11:56:23 AM
Last activity Apr 22, 2020 2:24:57 PM

Tags: Investigate with flows
Firmware Download, Start CPU, Stop CPU, Read Var, Write Var, S7Plus

✓ Approve activity | X Report activity

Show details

5 | -

These elements let us think that this is actually an attack. We report this issue and start to counter the attack immediately with the security team. If other suspicious changes happen, the Monitor mode will notify them.